

## Accepted Manuscript

Secure or usable computers? Revealing employees' perceptions and trade-offs by means of a discrete choice experiment

Eric Molin , Kirsten Meeuwisse , Wolter Pieters , Caspar Chorus

PII: S0167-4048(18)30239-6  
DOI: [10.1016/j.cose.2018.03.003](https://doi.org/10.1016/j.cose.2018.03.003)  
Reference: COSE 1309



To appear in: *Computers & Security*

Received date: 28 May 2017  
Revised date: 16 February 2018  
Accepted date: 18 March 2018

Please cite this article as: Eric Molin , Kirsten Meeuwisse , Wolter Pieters , Caspar Chorus , Secure or usable computers? Revealing employees' perceptions and trade-offs by means of a discrete choice experiment, *Computers & Security* (2018), doi: [10.1016/j.cose.2018.03.003](https://doi.org/10.1016/j.cose.2018.03.003)

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Secure or usable computers? Revealing employees' perceptions and trade-offs by means of a discrete choice experiment

Eric Molin, Associate Professor of Travel Behavior Research, Engineering Systems and Services Department, Faculty of Technology, Policy and Management, Delft University of Technology.

Kirsten Meeuwisse, Consultant Cyber Security, Deloitte.

Wolter Pieters, Associate Professor of Cyber Risk, Values, Technology and Innovation Department, Faculty of Technology, Policy and Management, Delft University of Technology.

Caspar Chorus, Professor of Choice behavior modelling, Engineering Systems and Services Department, Faculty of Technology, Policy and Management, Delft University of Technology.

## ABSTRACT

It is often suggested in the literature that employees regard technical security measures (TSMs) as user-unfriendly, indicating a trade-off between security and usability. However, there is little empirical evidence of such a trade-off, nor about the strength of the associated negative correlation and the importance employees attach to both properties. This paper intends to fill these knowledge gaps by studying employees' trade-offs concerning the usability and security of TSMs within a discrete choice experiment (DCE) framework. In our DCE, employees are asked to indicate the most preferred security packages that describe combinations of TSMs. In addition, security and usability perceptions of the security packages are explicitly measured and modelled. The models estimated from these observed responses indicate how each TSM affects perceived security, perceived usability and preference. The paper further illustrates how the modelling results can be applied to design highly secure packages that are still preferred by employees. The paper also makes a methodological contribution to the literature by introducing discrete choice experiments to the field of information security.

Keywords

Information security; Security measures; Security perception; Usability perception; Discrete choice experiments; Discrete choice models; Employees' preferences

## 1. Introduction

More than 40 million cybersecurity incidents are reported every year, and the damage done by cybercrime to the private sector is estimated to amount to hundreds of billions of euros every year (ISACA, 2015; Gandal, 2015). These numbers indicate that information security is of utmost importance for companies. Companies protect themselves from data breaches and cyberattacks by implementing a range of technical security measures (TSMs). If employees use these measures as intended, more stringent security measures would by design result in higher levels of security, although they may have a negative impact on productivity. However, if employees perceive those measures as less usable they may find ways to circumvent them, which potentially makes them less or even counter-effective (Dinev et al., 2006; Kirlappos et al., 2015; Post and Kagan, 2007). For example, if employees are forced to change their password every week, they may write down their passwords on post-its attached to their desk. Although it is usually the companies' Chief Information Security Officer (CISO) who makes the decisions on technical security measures, it is the compliance

Download English Version:

<https://daneshyari.com/en/article/6883836>

Download Persian Version:

<https://daneshyari.com/article/6883836>

[Daneshyari.com](https://daneshyari.com)